Peter C. Hildreth
*Bank Commissioner*

Robert A. Fleury
*Deputy Bank Commissioner*

64B Old Suncook Road
Concord, NH 03301

Phone (603) 271-3561

*Division FAX Numbers:*
Banking (603) 271-1090
Consumer Credit (603) 271-0750

*The*
# BANKING DEPARTMENT NEWSLETTER
WINTER 2006

www.nh.gov/banking

**Volume 5 • Issue 1**

## FROM THE COMMISSIONER'S DESK

Welcome to the first Banking Department newsletter of 2006. We have a lot of interesting information in this issue; but I would like to highlight several items.

Under the Legislative Update, there are two important pieces of legislation for you to consider. First, the issue of identity theft and breach of privacy generated a lot of different bills. HB 1660 was the vehicle used to address this important area of what we all do. Second, SB 394, the Trust Modernization and Competitiveness Act, will make major changes in trust company law and the trust law in general. If you are involved in trusts and haven't seen this legislation, you should review the latest version. Both of these bills can be found on the legislative website www.gencourt.state.nh.us.

I hope you enjoy this newsletter. If you need more information or assistance with any of the issues discussed in this issue, please feel free to contact us.

## BANKING DIVISION NEWS

*Charles M. O'Connor – Chief Bank Examiner*

### New Procedures for Suspicious Activity Reporting to the Banking Department

In January 2006, the New Hampshire Banking Department (NHBD) obtained authorization to access FinCEN's secure web-based environment aptly named BSA Direct. Access to the database will allow the review of CTR and SAR filings online in conjunction with any off-site review. The new technology is anticipated to enhance and support the BSA review process by allowing the user to compare and review multiple sources of information.

New Hampshire RSA 384:36 – Reports of Proscribed Activity requires that state chartered financial institutions concurrently file a *paper* copy of any SAR to the Commissioner of the New Hampshire Banking Department (NHBD) when such a report is submitted to that institution's federal regulator. However, for any New Hampshire institution reporting SARs to FinCEN using BSA Direct E-filing, an alternate manner of notification to the NHBD is now available.

Any New Hampshire state chartered institution reporting SARs to FinCEN may now notify the NHBD via a link found on the Banking Department's website. Upon submitting your SAR report to FinCEN, just connect to http://www.nh.gov/banking/banking.html, click on the "Notice of FinCEN Filing" link, complete the form, and submit. If your institution notifies the NHBD by this electronic process, a paper copy of the SAR does not need to be filed with the NHBD.

For further information or clarification on this change, don't hesitate to contact us.

### FinCEN Moving Forward with BSA Direct E-filing

According to the Financial Crimes Enforcement Network (FinCEN), over 15 million BSA reports (including Cash Transaction Reports (CTRs) and Suspicious Activity Reports (SARs) are filed each year by more than 25,000 U.S. financial institutions. These reports provide information to governmental and law enforcement agencies which are tasked to detect, investigate and ultimately deter criminal and terrorist activity.

Prior to 1990 and continuing to the present, in cooperation with FinCEN, an electronic system maintained by the Detroit Computing Center of the Internal Revenue Service has received paper copies and magnetic tapes of various reports, such as the CTRs and SARs. Upon receipt, the Detroit center would then convert these reports into electronic data. As a repository for this information, the Detroit center would also request, collect, and amend reported data through correspondence generated by the center. The process to collect/convert the paper documents and magnetic tapes into electronic data has been immense.

Section 361 of the USA Patriot Act of 2001 requires FinCEN to "establish and maintain a government-wide data access service, with access to … information collected by the Department of the Treasury, including report information" such as CTRs and SARs.

In response to the Section 361 mandate, FinCEN launched the Patriot Act Information System (PACS) in 2002. PACS, now known as BSA Direct E-filing (BSA Direct) allows participating institutions to file reports utilizing the Internet. This is a faster, less costly, and more efficient manner of delivery.

FinCEN's BSA Direct secure web-based system enables institutions to file the required reports electronically. The system also allows the reports to be accessed by authorized regulatory and law enforcement agencies.

FinCEN is working diligently to transition from having reports flow through the IRS Detroit center to fully implement the BSA Direct system for all report filers. It is anticipated that by year end 2006, 40% of all reports will be filed through the new BSA Direct E-filing program.

Given the pace of this transition, your institution may be filing online soon. After all, BSA Direct E-filing is only a click away!

To learn more about BSA Direct E-filing access FinCEN at http://www.fincen.gov.

## Account Review Programs

*By Chris Blanchette, Bank Examiner IV*

An effective account review program is an integral part of a strong trust risk management program. It also serves as a management tool to help ensure that all fiduciary responsibilities are sufficiently met. Not only should the account reviews help to determine compliance with an account's investment objectives, administrative duties also need to be evaluated as part of a comprehensive review program and to reduce exposure to potential liability.

A comprehensive account review includes both an administrative and an investment review. The scope of each review is dependent upon the fiduciary responsibilities and types of accounts. The board of directors is responsible for ensuring account reviews are completed; however, it may delegate the account review function to a subcommittee or independent trust officer. Smaller departments and trust companies should attempt to make the review process as independent as possible given the available resources. Ideally, an independent person should be performing the actual reviews before submission to a committee, but the other school of thought is that trust officers should be performing the review before submission to a committee since he/she should be the most knowledgeable on each account. Some larger trust departments have a completely independent review function separate from the trust officers. Nonetheless, the effectiveness of the program is more important than the manner in which the review process is conducted.

The Statement of Principles of Trust Department Management requires that all trust accounts be reviewed during each calendar year. The administrative and investment reviews need to be completed during each calendar year for all accounts with full fiduciary capacities (i.e. trustee, co-trustee, successor trustee, etc.). For accounts with investment discretion, such as trust agency or investment management accounts, the investment review needs to be completed during each calendar year; however, the administrative review may be done less frequently for lower risk accounts. Custodial accounts should also have an administrative review completed in order to ensure the accounts are being administered in accordance with signed agreements. This also applies for ERISA employee benefit plans and self-directed IRAs as they are considered trust accounts under Internal Revenue Code Section 408(h). Alternatively, accounts that are determined to be problematic or labor intensive may require more frequent reviews to help ensure fiduciary compliance. Examples of these types of accounts include accounts involving pending litigation, complaints from grantors or beneficiaries, or invest in complex and/or high risk investments.

Refer to the Trust Examination Manual, which is available at www.fdic.gov, for further details. Click on "Account Review Program" under the Management section of the manual. Examples of what types of items should be included in administrative and investment reviews can be found there. Although the lists are not intended to be all-inclusive, they are good starting points in the development of an effective account review program. Management should customize the reviews in order to meet the needs of the institution, as well as ensure the board of directors that all fiduciary obligations are being satisfied.

## Authentication

*By Parker T. Howell, Bank Examiner IV*

### Introduction

Passwords are the most common form of authentication, and password requirements are becoming more and more stringent. Users are trying to strike the right balance between password length, complexity, and the ability to remember them. Where does the balance lie? Password cracking programs are becoming stronger and faster, rendering even complex passwords vulnerable to compromise. Will

passwords become a thing of the past? I will try to answer these questions and provide some background on authentication and current password best practices.

**Authentication**

The term authentication as used in this document is the process of verifying the identity of a person or entity, then using the process to control access to data and resources.

Types of authentication techniques include:

- Something you know: Passwords and PIN's
- Something you have: Smart Cards, Tokens, Digital Certificates
- Something you are: Signature, Biometrics

Multi-factor authentication is a combination of any two or more. For instance ATM cards use something you have (card) and something you know (PIN). Multi-factor authentication does not include using two different passwords. This is known as layered security.

**So what kind of authentication should you use?**

True to examiner style I will tell you that it depends on the information you are trying to protect. As I stated in the last newsletter, the more sensitive or confidential the information is, the stronger the safeguard should be. This goes back to the risk assessment. What are you trying to protect, and how sensitive is it? The more sensitive the information the stronger the authentication needs to be. In almost every institution the password is one of the most critical and only security controls; and provides a crucial layer of defense. Unfortunately many passwords are weak, and can therefore be easily cracked, guessed, or stolen.

**FFIEC Guidance on Authentication in an Internet Banking Environment**

In October 2005, the FFIEC issued new guidance on authentication in an Internet Banking Environment. So what does that mean to you? In summary, the basic rule of thumb is; if non-public customer/member information is being transmitted via the Internet, then you should use multi-factor authentication. This not only applies to online banking and bill pay products, (which most institutions are reliant upon the vendor) but to remote access, and secure web servers. For instance, if an institution is allowing employees to work from home using a VPN connection, and they have access to non-public customer/member information, then multi-factor authentication should be used. If the Board of Directors accesses a secure website that contains non-public customer/member information then multi-factor authentication should be used. Full implementations of multi-factor authentication techniques are expected by year end 2006.

**Password Best Practices**

Provided below are current best password practices as recommended by Microsoft. Other sources may vary. Furthermore, these are minimum standards, are always changing, and are not a hard and fast rule.

- Include authentication practices in policy.
- Make sure that you always change default passwords and usernames as well as vendor supplied passwords and usernames. These are common targets for hackers.
- Password length – Minimum **8** characters with complexity requirements
- Password Change Frequency – **90** days
- Password Lockout Rule – **3**
- Passwords Remembered – **24**
- User Training!

**Summary**

Every time you provide a password or PIN to someone or something you are authenticating to them. Authentication provides a means to control access to systems. Passwords are the most popular form of authentication; however, they are the weakest. Other forms of authentication are inherently stronger than passwords but may be more difficult to implement; yet, they do provide for better security and can be easier to use if implemented properly. FFIEC guidance requires multi-factor authentication for high risk transactions. More information on authentication can be found in the FFIEC's Information Security Handbook at www.ffiec.gov.

## Overdraft Charges

*By Anne J. Rabuck, Staff Attorney*

The Banking Department has received several complaints from individuals regarding the assessment of overdraft charges to their checking accounts.

A typical scenario is as follows: A checking account with a balance of $500 is assessed four $25 fees ($100) for overdrawing the account when the financial institution posts five checks to the account that day in the following order: Check 1 for $475, Check 2 for $30, Check 3 for $60, Check 4 for $15 and Check 5 for $50.

However, if those same five checks, all of which were posted to the account that same day, were instead posted in this order: Check 2 for $30, Check 3 for $60, Check 4 for $15, Check 5 for $50 and Check 1 for $475, only one $25 overdraft fee would result.

It is true that the largest check is often an important payment that the customer would like to have the funds to satisfy. It is also true that in most account agreements there is a provision giving the financial institution authority to post checks in the order the financial institution chooses. Unfortunately, many financial institution customers aren't aware of this provision until they have been assessed with what are sometimes substantial fees.

Overdraft protection addresses the issue, but for those customers who do not have it, a separate disclosure of the account agreement's provisions regarding overdraft fees would draw attention to the issue and make it plain how these overdraft fees are assessed.

## LEGISLATIVE UPDATE

*Donna M. Soucy – General Counsel*

### Interim Rules Adopted

The Department recently adopted interim rules applicable to all licensees. These rules, Ban 2400 General Requirements: Licensees and Ban 2500 Mortgage Bankers and Brokers, can be found on our web site, http://www.nh.gov/banking/mortgagelr.html. For the most part, the existing rules were readopted. However, some changes were made to the application form. In addition, the requirement for personal financial disclosures was eliminated. The rules were adopted by the Commissioner and became effective on February 2, 2006. These rules will remain in effect until August 1, 2006. The Department has begun working on permanent rules. Please check our website and future editions of this newsletter for more information regarding rulemaking.

### Legislation to Watch

The Banking Department is currently monitoring a number of bills that could potentially affect the Department and/or the entities we regulate. There are two important bills however, that we chose to highlight in this edition of our newsletter.

The first bill is **HB 1660, regulating identity theft**. Although several pieces of legislation were introduced to address this issue, the House Commerce committee decided to adopt one comprehensive bill dealing with all of the issues raised relative to identity theft. HB 1660 as amended would require, "Any person doing business in this state who owns or licenses computerized data that includes personal information shall, when it becomes aware of a security breach, promptly determine the likelihood that the information has been or will be misused. If the determination is that misuse of the information has occurred or is reasonably likely to occur, or if a determination cannot be made, the person shall notify the affected individuals as soon as possible as required under this subdivision." The disclosure needs to be made as expediently as possible, but no more than 15 business days after the breach is discovered. The legislation also requires that entities regulated by the Banking Department notify the Department of the anticipated date of notice to individuals as well as the number of individuals who will be notified.

The House voted to adopt HB 1660 as amended on Wednesday, February 15, 2006. However, a floor amendment was also adopted to change the notification time to 3 days from discovery of the breach. The bill will now move to the Senate for further consideration.

The second piece of legislation, **SB 394, establishing the Trust Modernization and Competitiveness Act**, is still being considered by the Senate Judiciary Committee. This legislation and the amendment proposed at the hearing make significant changes to the trust company statute as well as the uniform trust code. The bill, which was filed at the behest of Trust New Hampshire First, LLC, makes a number of changes to the formation for process for trust companies and would allow for the formation of "Family Fiduciary Services Companies," companies that serve one or more family members and do not transact business with the general public.

At the request of the Banking Department, the amendment to the bill includes the following provisions:

- ***Capital***
  - increase capital to a minimum of $500,000 and require pledge of securities or a surety bond;
  - require maintenance of that level; and
  - provides a phase in period for existing trust companies to reach the $500,000 threshold.
- ***Increase Petition Fee*** – to $5,000 to better reflect the actual cost to the department of reviewing and examining the petitions.
- ***Information Sharing*** – although the bill includes significant confidentiality provisions, language was added to ensure that information can be shared with other state and federal regulators.
- ***Overall Modernized Language*** – updated and modernized the language of the statute to better reflect the current practices of the industry.

The proposed amendment to the bill has to be voted on by the Senate Judiciary Committee and then approved by the full Senate. If the legislation is adopted by the Senate it will then be forwarded to the House for their consideration.

# CONSUMER CREDIT DIVISION NEWS

*Mary L. Jurta – Director of Consumer Credit*

## Ameriquest Settlement Press Release

Banking Commissioner Peter C. Hildreth and Attorney General Kelly A. Ayotte announced on January 23, 2006 that Ameriquest Mortgage Company, the nation's largest sub-prime lender, has agreed to pay $295 million to consumers and make sweeping reforms of practices that states alleged amounted to predatory lending. Ameriquest also will pay a total of $30 million to the 49 states and D.C. that are participating in the settlement agreement for costs of the investigation and consumer education and enforcement.

Individual states' exact share of restitution funds has not been determined, but a reasonable estimate is that New Hampshire's share will be about $1,720,401.

The press release can be viewed at http://www.nh.gov/banking/PressReleaseAmeriquest.pdf

## Common Consumer Complaints – Consumer Credit Division

*By Andrea J. Shaw, Staff Attorney*

Licensees often ask the Department about the type of complaints we receive from consumers. The issues that consumers complain about vary greatly from complaint to complaint. The common denominator among most complaints is poor communication.

A majority of the consumer inquiries I receive are from consumers wondering if they were treated correctly and fairly. I purposefully used the term "consumer inquiry". This is the term that is actually used throughout the Consumer Credit Division Statutes (361-A:4-a, 397-A:15-a, 397-B:7, 399-A9, and 399-D:19) governing formal consumer inquiries to the Department. This is a more accurate term than "consumer complaint" because in half of the initial phone inquires the consumers are unsure if they have a complaint, but they have questions about their recent or ongoing financial transaction.

To lessen your company's chance of receiving consumer inquires, it is essential that your front line employees (such as loan originators, or those who arrange the automobile financing) receive training on how to educate the consumer about the financial transaction. The first step is for your front line employees to understand the products your company offers. Only when your employees are properly trained to understand the products can they begin to communicate effectively to the consumers regarding those products.

If you train your employees about your products and encourage clear communication with your customers, you will substantially reduce your company's chance of receiving consumer inquiries from the Department.